3 システムのセットアップ

購入後、初めて本製品をセットアップする時の手順を説明します。

セットアップの準備

セットアップには、本体以外のマシンや接続のためのケーブルなどが必要となります。また、それぞれのマシンについてもソフトウェアのインストールなどの準備が必要となります。

- **本体**

  購入時のハードディスク上にはファイアウォールのモジュール、および基本設定ツールがインストール済みです。これらを使用して、コンフィグレーションをしてください。

- **管理クライアント**

  システムの基本設定をするために使用する管理コンピュータとして使用します。
  設定ツール(Management Console)にアクセスするためのブラウザがインストールされていることを確認してください。ブラウザにはInternet Explorer 6.0 SP1(日本語版・Windows版)を推奨します。

- **ライセンスキー**

  本製品のセットアップには、ライセンスキーが必要となります。セットアップの前に準備してください。入手方法については、1章の「ライセンスキー」を参照してください。

セットアップ

本製品のセットアップについて順を追って説明します。

設定手順の流れ

設定手順の流れを以下に示します。

1. 初期導入設定用ディスクによる設定

1. 初期導入設定用ディスクの作成
2. 初期導入設定用ディスクによるセットアップ

2. システムの基本設定

3. かんたん設定によるセットアップ

4. バックアップ

1. システム基本情報のバックアップ
2. セキュリティポリシーのバックアップ

5. ESMPRO/ServerAgentのセットアップ

6. マザーボード情報のバックアップ

初期導入設定用ディスクによる設定

初期導入設定用ディスクでの設定方法について説明します。

初期導入設定用ディスクの作成

「初期導入設定用ディスク」はExpress5800/SG300をネットワークに接続するために必要な設定情報を保存したセットアップ用ディスクです。
添付の「初期導入設定用ディスク」にあらかじめ入っている「初期導入設定ツール」を使用して作成します。「初期導入設定ツール」は、Windows 98/NT4.0/2000/XPが動作するコンピュータで動作します。

初期導入設定ツールの実行と操作の流れ

次の順序で初期導入設定用ディスクを作成します。それぞれの設定項目については、この後に説明しています。

1. 管理クライアントマシンのフロッピーディスクドライブに添付の「初期導入設定用ディスク」をセットする。

2. フロッピーディスクドライブ内の「初期導入設定ツール(StartupConf.exe)」を実行する。

   「初期導入設定ツール」が起動します。

3. 開始画面が表示されたら[次へ]をクリックし、設定の入力を開始する。

   プログラムは、ウィザード形式となっており、各ページで設定に必要事項を入力して進んでいきます。必須項目が入力されていない場合や入力情報に誤りがある場合は警告メッセージが表示されますので、項目を正しく入力し直してください。入力事項の詳細については、後述の説明を参照してください。すべての項目の入力が完了すると、フロッピーディスクに設定情報を書き込んで終了します。

4. 初期導入設定用ディスクをフロッピーディスクドライブから取り出し、「初期導入設定用ディスクによるセットアップ」に進む。

重要 **初期導入設定用ディスクは再セットアップの際にも使用します。大切に保管してください。**

入力項目の設定

以下のネットワーク構成を例にして「初期導入設定ツール」で入力する項目について説明します。

設定項目表

初期導入設定用ディスクを作成する際に必要となる項目の一覧です。前ページのネットワーク構成例を元に本手順で設定する内容を設定例欄に記入してあります。

実際に使用されるネットワーク環境に即した内容を、該当する項目のお客様記入欄に記入し、以降の手順でExpress5800/SG300本体を設定する際に参照してください。

<table>
<tr><th>設定項目</th><th colspan="2">詳細設定項目</th><th>設定例</th><th>お客様記入欄</th></tr>
<tr><td rowspan="5">ネットワーク
インタフェース
の設定①</td><td colspan="2">ホスト名</td><td>firewall.nec.co.jp</td><td></td></tr>
<tr><td rowspan="2">内側ネットワーク</td><td>IPアドレス</td><td>192.168.1.126</td><td></td></tr>
<tr><td>ネットマスク</td><td>255.255.255.0</td><td></td></tr>
<tr><td rowspan="2">外側ネットワーク</td><td>IPアドレス</td><td>202.247.5.126</td><td></td></tr>
<tr><td>ネットマスク</td><td>255.255.255.0</td><td></td></tr>
<tr><td rowspan="4">ネットワーク
インタフェース
の設定②</td><td rowspan="2">DMZ</td><td>IPアドレス</td><td>172.16.1.126</td><td></td></tr>
<tr><td>ネットマスク</td><td>255.255.255.0</td><td></td></tr>
<tr><td rowspan="2">予備ネットワーク</td><td>IPアドレス</td><td></td><td></td></tr>
<tr><td>ネットマスク</td><td></td><td></td></tr>
<tr><td rowspan="4">ルーティングの
設定</td><td>デフォルトゲート
ウェイ</td><td>IPアドレス</td><td>202.247.5.254</td><td></td></tr>
<tr><td rowspan="3">静的ルーティング</td><td>IPアドレス</td><td></td><td></td></tr>
<tr><td>ネットマスク</td><td></td><td></td></tr>
<tr><td>ゲートウェイ</td><td></td><td></td></tr>
<tr><td rowspan="3">ネームサーバ
NTPサーバ
の設定</td><td>ネームサーバ 1</td><td>IPアドレス</td><td></td><td></td></tr>
<tr><td>ネームサーバ 2</td><td>IPアドレス</td><td></td><td></td></tr>
<tr><td>NTPサーバ</td><td>IPアドレス</td><td></td><td></td></tr>
<tr><td rowspan="3">リモートメンテ
ナンス機能の
設定</td><td colspan="2">管理者のメールアドレス</td><td>admin@nec.co.jp</td><td></td></tr>
<tr><td>メールゲート
ウェイ</td><td>IPアドレス</td><td></td><td></td></tr>
<tr><td>TRAP送信先
ホスト</td><td>IPアドレス</td><td></td><td></td></tr>
<tr><td rowspan="4">Management
Console
の設定</td><td colspan="2">ポート番号</td><td>18000</td><td></td></tr>
<tr><td colspan="2">管理者アカウント</td><td>admin</td><td></td></tr>
<tr><td colspan="2">パスワード</td><td></td><td></td></tr>
<tr><td colspan="2">パスワード（確認用）</td><td></td><td></td></tr>
</table>

設定項目	詳細設定項目	設定例	お客様記入欄
SSHに関する設定	Secure Shell (SSH)を使用する	オン	
	ポート番号	18022	
	管理者アカウント	admin	
	パスワード		
	パスワード(確認用)		
管理クライアントの設定	接続元1 IPアドレス	192.168.1.10	
	接続元2 IPアドレス		
	接続元3 IPアドレス		
	接続元4 IPアドレス		
二重化のセットアップ	二重化構成で使用する	オフ	
キーの入力	ライセンスキー1		
	ライセンスキー2		
	サポートキー1		
	サポートキー2		

● **ネットワークインタフェースの設定**

Express5800/SG300のネットワークの設定をします。

— ホスト名(必須項目)

ホスト名はドメイン名まで含めたFQDNの形式で入力してください。

— 内側IPアドレス(必須項目)

内側IPアドレスを入力します。

— 内側ネットマスク(必須項目)

内側IPアドレスに対するサブネットマスクを入力します。

— 外側IPアドレス(必須項目)

外側IPアドレスを入力します。

— 外側ネットマスク(必須項目)

外側IPアドレスに対するサブネットマスクを入力します。

各ネットワークインタフェースが、本装置のどのLANポートに相当しているかを下図に示します。

● **ネットワークインタフェースの設定**

非武装地帯(DMZ)を構成するネットワークと予備ネットワークの設定をします。

— DMZ IPアドレス

DMZ用IPアドレスを入力します。

— DMZネットマスク

DMZ用IPアドレスに対するサブネットマスクを入力します。

— 予備IPアドレス

予備として用意されている本装置の4番目のネットワークポートのIPアドレスを入力します。内部ネットワークでもうひとつのセグメントを用意する場合や、二重化構成時にサーバ間監視専用インタフェース(ハートビート)として使用します。

— 予備ネットマスク

予備IPアドレスに対するサブネットマスクを入力します。

各ネットワークインタフェースが、本装置のどのLANポートに相当しているかを下図に示します。

● **ルーティングの設定**

ルーティングの設定をします。静的ルーティングはここでは1つのみ設定可能です。リモート管理端末が内部の別ネットワークに存在する場合は静的ルーティングを指定してください。通常、運用に必要なルーティングはExpress5800/SG300の起動後にManagement Consoleから設定してください。

— デフォルトゲートウェイ(必須項目)

デフォルトゲートウェイのIPアドレスを設定します。

— 静的ルーティング

宛先ネットワークアドレスとネットマスクおよびゲートウェイの組み合わせを指定します。

● **ネームサーバ/NTPサーバの設定**

ネームサーバ/NTPサーバの設定をします。

— ネームサーバ1 IPアドレス

ネームサーバ1のIPアドレスを入力します。

— ネームサーバ2 IPアドレス

ネームサーバ2のIPアドレスを入力します。

— NTPサーバIPアドレス

NTPサーバのIPアドレスを入力します。

● **リモートメンテナンス機能の設定**

メールアドレスとリモートメンテナンス機能の利用に関する設定をします。

— 管理者のメールアドレス(必須項目)

管理者のメールアドレスを指定します。

— メールゲートウェイの設定

メールゲートウェイのIPアドレスを入力します。

メールゲートウェイのIPアドレスを省略した場合、システムが発信するメールはローカルのrootユーザ宛てに配送されます。

— TRAP送信先ホストIPアドレスの設定

SNMPのTRAP送信先ホストを設定します。

● **Management Consoleに関する設定**

Management Consoleに関する設定をします。

— ポート番号(必須項目)

Management Consoleで使用するポート番号を入力します。規定値は、18000です。必要に応じて変更してください。

— 管理者アカウント名(必須項目)

管理クライアントからManagement Consoleに接続する際の管理者名(15文字以内)を入力します。

— パスワード(必須項目)

管理者に対する、パスワードを設定します。

— パスワードの再入力(必須項目)

確認のため、パスワードを再度入力します。

● **SSHに関する設定**

SSHに関する設定をします。

— Secure Shell(SSH)を使用する

使用する場合:
　チェックボックスをチェック
使用しない場合:
　チェックボックスのチェックをはずす。

— ポート番号

SSHで使用するポート番号を入力します。既定値は18022です。必要に応じて変更してください。

— 管理者アカウント名

管理クライアントからSSHで接続する際の管理者名(15文字以内)を入力します。

— パスワード

管理者に対する、パスワードを設定します。

— パスワードの再入力

確認のため、パスワードを再度入力します。

● 管理クライアントの設定

Express5800/SG300が接続を許可する管理クライアントのIPアドレスを登録します。

［接続元1 IPアドレス］は入力必須の項目です。残りのIPアドレスは必要に応じて登録してください。

接続元のIPアドレスは、Management Consoleから追加登録することができます。Management Consoleにログイン後、[Management Console]→[リモートメンテナンス]の順に進むと設定画面が表示されます。

● 二重化のセットアップ

2台のExpress5800/SG300を使用して可用性を高めることができます。二重化を構築する場合は、［設定対象ホストを二重化構成で使用する］にチェックしてください。二重化構成の詳細については、この章の「二重化構成について」で説明しています。

二重化構成で使用する場合、相手となるExpress5800/SG300の初期導入用設定ディスクの作成の際にもチェックを入れておくことをお勧めします（ただし、二重化の設定は後からでもできます）。

● ライセンスの設定

Express5800/SG300をファイアウォールとして使用するために、この画面で入手しているライセンスキーを入力してください。

また、ソフトウェアサポートサービスの契約をしている場合は、発行されたサポートキーを併せて入力します。

ライセンスキー、およびサポートキーの詳細については、1章の「ライセンスキー」、および「ソフトウェアサポート」を参照してください。

ライセンスキー、およびサポートキーは、初期導入設定用ディスクによる設定の後、Management Consoleからも登録することができます。Management Consoleにログイン後、[ファイアウォール]→[ライセンス確認/登録]の順に進むと登録画面が表示されます。

初期導入設定用ディスクによるセットアップ

初期導入設定ツールで作成した「初期導入設定用ディスク」を使用してセットアップし、管理クライアントをExpress5800/SG300へ接続します。

セットアップ手順

以下の手順でセットアップします。
正しくセットアップできないときは、この後の「セットアップに失敗した場合」を参照してください。

1. Express5800/SG300の電源がOFFの状態で、管理クライアントとExpress5800/SG300背面にあるLANポートインタフェース(内部ネットワーク用)をクロスケーブルで接続するか、Express5800/SG300が接続されている内部ネットワークのハブなどに管理クライアントのLANケーブルを接続する。

2. 初期導入設定用ディスクをExpress5800/SG300のフロッピーディスクドライブにセットする。

3. 本体のPOWERスイッチを押し、POWERランプが点灯することを確認する。

   しばらくすると、初期導入設定用ディスクから設定情報を読み取り、自動的にセットアップを進めます。2〜3分ほどでセットアップが完了します。

4. 管理クライアントのブラウザを使用して、Express5800/SG300のManagement Consoleへ接続する。

   重要

   Management Consoleには必ず内部ネットワークの管理クライアントから接続するようにしてください。外部から接続を許可する設定には絶対にしないでください。また、Management Consoleを使用する場合は、Internet Explorer 6.0 SP1(日本語版・Windows版)以上を使用してください。

   このときのURLには、Express5800/SG300の内側(管理クライアントが設置されているネットワーク側)のインタフェースのIPアドレスと初期導入設定ツールで設定したポート番号を指定します。

   接続すると、セキュリティの警告が表示されます。

5. [はい]をクリックする。

6. 初期導入設定ツールで設定した管理者アカウント名とパスワードを入力する。

   接続に成功すると、Management Consoleのログイン画面が表示されます。

7. [システム管理者ログイン]をクリックする。

   Management Consoleのトップ画面が表示されます。

8. 左側のメニューの[基本設定]アイコンをクリックする。

   初期導入設定ツールで設定した内容が正しく表示されていることを確認してください。

これで初期導入設定用ディスクによるセットアップ、管理クライアントの接続は完了です。以降の説明では、管理クライアントからの操作でシステムのセットアップを行います。

セットアップの完了が確認できたらセットした初期導入設定用ディスクをフロッピーディスクドライブから取り出して大切に保管してください。再セットアップの時に使用することができます。

上記の画面上で設定を変更することができますが、変更する前に後述の「システムの基本設定」の説明をよくお読みください。この画面で設定項目とその説明があります。

セットアップに失敗した場合

システムのセットアップに失敗した場合は、自動的に電源がOFF(POWERランプ消灯)になり、ユーザーに異常終了したことを知らせます。正常にセットアップを完了できなかった場合は、初期導入設定用ディスクに書き出されるログファイル「logging.txt」の内容を確認し、再度初期導入設定ツールを使用して初期導入設定用ディスクを作成してください。

〈主なログの出力例〉

「Error: cannot open: /mnt/floppy/fwsinit.ini」

→ 初期導入設定用ディスク中の設定に誤りがある場合に表示されます。

「Error: bad user name (WbMC)」

→ 初期導入設定用ディスク中のManagement Consoleの管理者名の指定に誤りがある場合に表示されます。

「Error: bad user name (SSH)」

→ 初期導入設定用ディスク中のSSHの管理者名の指定に誤りがある場合に表示されます。

「Error: port number of WbMC and SSH is the same.」

→ Management Consoleのポート番号とSSHのポート番号に同一の値が設定された場合に表示されます。Management Consoleのポート番号とSSHのポート番号には違う値を設定する必要があります。

「Error: fwsetup failure.」

→ ファイアウォールへ初期導入設定ができない場合に表示されます。初期導入設定用ディスクの設定に誤りがあります。

初期導入設定用ディスクの内容が誤っていた場合、初期導入設定用ディスクの設定内容を修正して再度セットアップすることができます。
ただし、以下の操作を行った場合には、初期導入設定用ディスクによる設定の機能はOFFになります。設定の変更が、基本設定ツール(sgsetup)もしくはManagement Consoleからしかできなくなりますので注意してください。

- Management Consoleの基本設定画面から[設定]をクリックした場合。
- コンソールから基本設定ツール(sgsetup)を実行した場合。

システムの基本設定

前述の「初期導入設定用ディスクによる設定」で管理クライアントからExpress5800/SG300に接続するための最低限必要なセットアップが完了しました。ここからは、Management Consoleを使用して、さらに詳細なセットアップを行います。
以下にManagement Consoleを使用した基本設定の項目や実際の手順の流れを示します。

Management Consoleには必ず内部ネットワークの管理クライアントから接続するようにしてください。外部から接続を許可する設定には絶対にしないでください。また、Management Consoleを使用する場合は、Internet Explorer 6.0 SP1(日本語版・Windows版)以上を使用してください。

1. 管理クライアントのウェブブラウザを使用して、Express5800/SG300のManagement Consoleに接続する。

   このときのURLには、Express5800/SG300の内側(管理クライアントが設置されているネットワーク側)のインタフェースのIPアドレスと初期導入設定ツールで設定したポート番号を指定します。

   接続すると、セキュリティの警告が表示されます。

2. [はい]をクリックする。

3. 初期導入設定ツールで設定した管理者アカウント名とパスワードを入力する。

   接続に成功すると、Management Consoleのトップメニューの画面が表示されます。

4. 左側のメニューから[基本設定]アイコンをクリックする。

基本設定画面が表示されます。

5. 次の基本設定項目を設定する。

Express5800/SG300のホスト名、IPアドレス、ルーティングなどの初期導入設定用ディスクで設定した項目については、設定値を確認してください。

ヒント

- [ホスト名]と[インタフェース]、[デフォルトゲートウェイ]の項目の背景色が他と異なるのは、これらの項目を変更すると装置の再起動が必要となることを示しています。その他の項目は設定を変更しても、再起動をする必要はありません。
- 変更や追加した内容を破棄したい場合は、[元に戻す]をクリックして終了してください。

- ホスト名（FQDN）（必須項目）

  ホスト名を入力します。

- インタフェース（IPアドレス/ネットマスク/MTU値）（必須項目）

  各インタフェースのIPアドレス、ネットマスクおよびMTU値を入力します。各インタフェースが、本装置のどのLANポートに相当するかは51、52ページを参照してください。

- ネームサーバ

  ネームサーバのIPアドレスを入力します。（複数入力可）

- 管理者メールアドレス（必須項目）

  管理者のメールアドレスを指定します。

- メールゲートウェイ

  使用か未使用かを指定します。使用の場合は、メールゲートウェイのIPアドレスを入力します。

- デフォルトゲートウェイ（必須項目）

  デフォルトゲートウェイのIPアドレスを設定します。

- 静的ルーティング（アドレス/ネットマスク/ゲートウェイ）

  宛先ネットワークアドレスとネットマスクおよびゲートウェイの組み合わせを指定します。必要に応じてインタフェースを「自動」以外に変更し、関連付けたいインタフェースを指定します。

- トラップ送信先ホストのIPアドレス

  SNMPのTRAP送信先ホストを設定します。

- NTP時刻同期サーバ

  NTPサーバのIPアドレスを入力します。

- 二重化機能

  設定対象のホストを二重化構成で使用する場合は、［使用］を選択します。

6. 確認ができたら、[設定]をクリックする。

   操作結果画面が表示されます。

   操作結果画面は、設定内容がシステムの再起動後に有効になる場合と再起動を必要とせずに有効となる場合でメッセージが異なります。
   再起動を促す指示を含むメッセージが表示された場合は、手順7以降を参照して作業を続けてください。再起動の指示が含まれていない場合は、以上で基本設定は完了です。

再起動が必要

再起動は必要なし

7. [戻る]をクリックする。

8. 左側のメニューの[システム]アイコンをクリックし、[システムの再起動]をクリックする。

9. [OK]をクリックする。

10. [即再起動]をクリックし、再起動する。

これでシステムの基本設定は完了です。

セキュリティポリシーのセットアップ

次にネットワークを攻撃から守るための通信制御(以降、「セキュリティポリシー」と呼びます)を設定します。

かんたん設定ウィザードを実行すると、Express5800/SG300を導入するネットワーク環境に即した一般的なセキュリティポリシーを設定することができます。
Management Consoleの「ファイアウォール」メニューから[かんたん設定]をクリックして、Express5800/SG300を導入するネットワーク環境に合わせて、以下の各項で説明する内容を入力、または選択することにより、環境に即したセキュリティポリシーの設定ができます。

セキュリティポリシーの詳細な設定方法については、4章を参照してください。

公開サーバ設定項目表

かんたん設定ウィザードで設定する項目の一覧です。49ページのネットワーク構成例を元にここでの手順で設定する内容を設定例欄に記入しています。

実際に使用されるネットワーク環境に即した内容を、該当する項目のお客様記入欄に記入し、以降の手順でExpress5800/SG300本体を設定する際に参照してください。

設定項目		詳細設定項目	設定例	お客様記入欄
DMZ		あり/なし	あり	
アドレス変換		する/しない	する	
HTTPサーバ	1	公開IPアドレス	202.247.5.127	
		内部IPアドレス	172.16.1.10	
		ポート番号	80	
	2	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
	3	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
ウェブサーバ		公開IPアドレス	202.247.5.127	
		内部IPアドレス	172.16.1.10	
メールサーバ		公開IPアドレス	202.247.5.128	
		内部IPアドレス	172.16.1.11	
ファイルサーバ		公開IPアドレス	202.247.5.127	
		内部IPアドレス	172.16.1.10	

<table>
<tr><th colspan="2">設定項目</th><th>詳細設定項目</th><th>設定例</th><th>お客様記入欄</th></tr>
<tr><td colspan="2" rowspan="2">ネームサーバ</td><td>公開IPアドレス</td><td>202.247.5.128</td><td></td></tr>
<tr><td>内部IPアドレス</td><td>172.16.1.11</td><td></td></tr>
<tr><td rowspan="15">その他のサーバ</td><td rowspan="3">1</td><td>公開IPアドレス</td><td></td><td></td></tr>
<tr><td>内部IPアドレス</td><td></td><td></td></tr>
<tr><td>ポート番号</td><td></td><td></td></tr>
<tr><td rowspan="3">2</td><td>公開IPアドレス</td><td></td><td></td></tr>
<tr><td>内部IPアドレス</td><td></td><td></td></tr>
<tr><td>ポート番号</td><td></td><td></td></tr>
<tr><td rowspan="3">3</td><td>公開IPアドレス</td><td></td><td></td></tr>
<tr><td>内部IPアドレス</td><td></td><td></td></tr>
<tr><td>ポート番号</td><td></td><td></td></tr>
<tr><td rowspan="3">4</td><td>公開IPアドレス</td><td></td><td></td></tr>
<tr><td>内部IPアドレス</td><td></td><td></td></tr>
<tr><td>ポート番号</td><td></td><td></td></tr>
<tr><td rowspan="3">5</td><td>公開IPアドレス</td><td></td><td></td></tr>
<tr><td>内部IPアドレス</td><td></td><td></td></tr>
<tr><td>ポート番号</td><td></td><td></td></tr>
<tr><td colspan="2" rowspan="5">内部からの利用を
許可するサービス</td><td>ウェブサービス
(HTTP/HTTPS)</td><td>許可する</td><td></td></tr>
<tr><td>メールサービス
(SMTP)</td><td>許可する</td><td></td></tr>
<tr><td>ファイル転送サービス
(FTP)</td><td>許可する</td><td></td></tr>
<tr><td>ネームサービス(DNS)</td><td>許可する</td><td></td></tr>
<tr><td>時刻同期サービス
(NTP)</td><td>許可しない</td><td></td></tr>
<tr><td colspan="2">不正アクセス対策</td><td>レベル</td><td>ベーシック</td><td></td></tr>
<tr><td colspan="2" rowspan="2">ユーザ認証</td><td>する/しない</td><td>しない</td><td></td></tr>
<tr><td>ポート番号</td><td></td><td></td></tr>
</table>

Management Consoleの起動

Express5800/SG300の内部ネットワークと接続している管理クライアントでウェブブラウザを起動し、Management Consoleに接続します(Management Consoleの接続については、前述の「システムの基本設定」を参照してください)。

ライセンスとソフトウェアサポートサービスの登録

ライセンスの登録を行います。すでに初期導入設定用ディスクによる設定でライセンスの登録を完了している場合は、本項目でのライセンス登録は必要ありません。かんたん設定ウィザードによるポリシールールの作成に進んでください。

重要 **ライセンスの登録をしていないと、Express5800/SG300は初期導入設定ディスクや基本設定で登録した内容のみが設定された装置にとしてしか使えません。ファイアウォールのサービスを提供することができません。**

ライセンスキー、サポートキーの取得については1章の「ライセンスキー」および「ソフトウェアサポートサービス」を参照してください。

1. Management Consoleの画面左側に並ぶメニューアイコンから[ファイアフォール]アイコンをクリックする。

2. 「ファイアウォール」メニューでライセンスの[確認/登録]をクリックする。

3. ライセンスキーを入力し、[登録]をクリックする。

   ライセンスの登録完了画面が表示されます。

新たにサポートライセンスを取得する場合は、ライセンスキーの情報が必要となります。
現在有効なキーは、以下のボタンを押すと確認できます。

有効なキーの表示

4. [ライセンス登録に戻る]をクリックする。

ライセンスキーを登録しました。

ライセンス登録に戻る

5. <ソフトウェアサポートサービスを購入している場合>

   サポートキーを入力し、[登録]をクリックする。

■ サポート期間
有効なサポートキーは登録されていません
■ ライセンスの登録
ライセンスキー
登録
サポートキー
登録

新たにサポートライセンスを取得する場合は、ライセンスキーの情報が必要となります。
現在有効なキーは、以下のボタンを押すと確認できます。

有効なキーの表示

   登録完了画面が表示されます。

2003年04月01日～2004年03月31日のサポートキーが有効となりました。

ライセンス登録に戻る

かんたん設定ウィザードによるポリシールールの作成

以下の各手順で入力する値には、63ページの公開サーバ設定項目表に記入したお客様記入欄の対応する項目の値を入力してください。

1. Management Consoleの画面左側に並ぶメニューアイコンから[ファイアフォール]アイコンをクリックする。

2. 「ファイアウォール」メニュー画面が表示されたら、[かんたん設定]をクリックし、かんたん設定ウィザードを実行する。

3. かんたん設定ウィザードを用いて設定した現在の設定内容を通知する設定内容確認画面が表示されたら、[再設定]をクリックする。

   インストール直後など、一度もかんたん設定ウィザードを利用したことがない場合には、設定内容確認画面は表示されず、次のネットワーク構成の選択に移ります。

4. 「DMZあり」にチェックをし、[次へ]をクリックする。

5. 各ネットワークアドレスを設定（本手順では「アドレス変換(NAT/NAPT)を行う」をチェック）して、［次へ］をクリックする。

6. 「公開するウェブサーバ(HTTP)はある」にチェックし、「公開IPアドレス」にウェブサーバとして公開するIPアドレス、「内部IPアドレス」にウェブサーバの実IPアドレスを記入して、［次へ］をクリックする。

7. 「公開するメールサーバ(SMTP)はある」にチェックし、「公開IPアドレス」にメールサーバとして公開するIPアドレス、「内部IPアドレス」にメールサーバの実IPアドレスを記入して、［次へ］をクリックする。

8. 「公開するファイル転送サーバ(FTP)はある」にチェックし、「公開IPアドレス」にファイル転送サーバとして公開するIPアドレス、「内部IPアドレス」にファイル転送サーバの実IPアドレスを記入して、［次へ］をクリックする。

外部へ公開する「ファイル転送サーバ(FTP)」はありますか？

戻る　次へ

○ 公開するファイル転送サーバ(FTP)はない

◉ 公開するファイル転送サーバ(FTP)はある

サーバ	公開IPアドレス	→	内部IPアドレス
1台目	202.247.5.127	→	172.16.1.10

9. 「公開するネームサーバ(DNS)サーバはある」にチェックし、「公開IPアドレス」にネームサーバとして公開するIPアドレス、「内部IPアドレス」にネームサーバの実IPアドレスを記入して、［次へ］をクリックする。

10. 外部へ公開するその他のサーバを設定（本手順では「その他の公開するサーバはない」を選択）して、［次へ］をクリックする。

11. 使用環境に合わせて利用するサービスを「利用する」に変更して、［次へ］をクリックする。

外部ネットワークに公開されている、どのようなサービスを利用しますか？

戻る　次へ

■ 利用するサービス	
ウェブサービス(HTTP/HTTPS)	◉利用する ○利用しない
メールサービス(SMTP)	◉利用する ○利用しない
ファイル転送サービス(FTP)	◉利用する ○利用しない
ネームサービス(DNS)	◉利用する ○利用しない
時刻同期サービス(NTP)	○利用する ◉利用しない

12. 不正アクセス対策レベルを指定(本手順では「ベーシック」を指定)して[次へ]をクリックする。

アドバンス(ベーシックを含む)

■ 通信流入量制限
外部からの過多アクセスからサーバを守ります。
■ 内部アドレスの隠蔽
内部ネットワークから外部へアクセスする際に発信元のアドレスを隠蔽することで内部ネットワークへの不正なアクセスを防止します。
■ オートディフェンス
ウェブ・メール各々の不正アクセスに対する応答を偽装し、不正アクセスから守ります。

上記の対策を行わない(問題がなければ 選択しないでください)

13. ユーザ認証に関する設定をして(本手順では「ユーザ認証を利用しない」を選択)、[次へ]をクリックする。

ユーザ認証を利用しますか？

戻る　次へ

ユーザ認証を利用しない

ユーザ認証を利用する

ユーザ認証ウェブのポート番号を 18080 とする
(分からない場合は、変更しないで下さい)

どこからの認証を許可しますか？
内部ネットワークからのみ許可する
すべてのネットワークから許可する

14. これまでの手順で設定した内容が正しく反映されていることを確認し、[設定]をクリックする。

設定内容に誤りがある場合は[やり直し]をクリックし、再度設定を行ってください。

下記のように設定してよろしいですか？

■アドレス変換を行う。
■不正アクセス対策(ベーシック)を行う。
■ユーザ認証を利用しない。

■ 外部ネットワーク上の利用可能サービス
ウェブサービス(HTTP/HTTPS)
メールサービス(SMTP)
ファイル転送サービス(FTP)
ネームサービス(DNS)

公開サーバ	公開IPアドレス	内部IPアドレス
ウェブサーバ(HTTP)	202.247.5.127	172.16.1.10:80
メールサーバ(SMTP)	202.247.5.128	172.16.1.11
ファイル転送サーバ(FTP)	202.247.5.127	172.16.1.10
ネームサーバ(DNS)	202.247.5.128	172.16.1.11

戻る　やり直し　設定

Express5800/SG300に設定内容が反映され、設定内容の画面が表示されます。

下記のように設定しました。

■アドレス変換を行う。
■不正アクセス対策(ベーシック)を行う。
■ユーザ認証を利用しない。

■ 外部ネットワーク上の利用可能サービス
ウェブサービス(HTTP/HTTPS)
メールサービス(SMTP)
ファイル転送サービス(FTP)
ネームサービス(DNS)

■ 外部ネットワークへ公開するサーバ		
公開サーバ	公開IPアドレス	内部IPアドレス
ウェブサーバ(HTTP)	202.247.5.127	172.16.1.10:80
メールサーバ(SMTP)	202.247.5.128	172.16.1.11
ファイル転送サーバ(FTP)	202.247.5.127	172.16.1.10
ネームサーバ(DNS)	202.247.5.128	172.16.1.11

かんたん設定を終了

バックアップ

システムのセットアップが終了した後、万一の故障による再セットアップに備えて、設定した情報のバックアップを作成します。

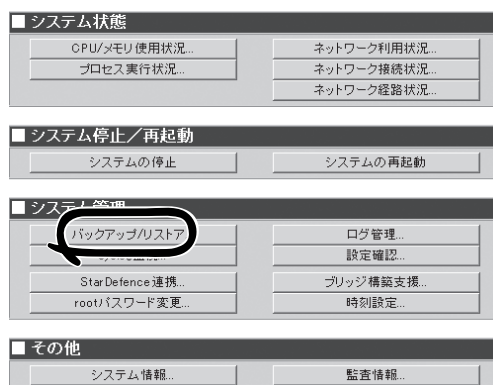
システム基本情報のバックアップ

Management Consoleを使って、システム基本情報をバックアップすることをお勧めします。
システム基本情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。

重要 **Management Consoleから操作し、バックアップを行います。Management Consoleへの接続については、4章を参照してください。**

システム基本情報は、管理クライアントへバックアップデータを保存します。

1. 管理クライアントのウェブブラウザを使用してExpress5800/SG300のManagement Consoleに接続し、左側のメニューから[システム]アイコンをクリックする。

2. [バックアップ/リストア]をクリックする。

3. バックアップ先を選択して、ボタンをクリックする。

4. [バックアップ]をクリックする。

二重化構成時(基本設定画面で二重化機能を[使用]するに設定した場合)は、バックアップ対象として[基本設定画面での設定内容を含める]を選択して、[バックアップ]をクリックしてください。

なお、運用系から待機系に設定を同期させるためのバックアップの場合は、[基本設定画面での設定内容を含めない]を選択して、[バックアップ]をクリックしてください。

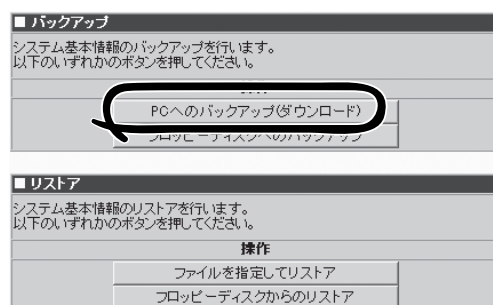
<二重化構成時>

❷ [バックアップ]をクリック　❶ バックアップ対象を選択

5. [保存]をクリックし、保存先を確認して、保存する。

6. 保存するディレクトリを選択し、ファイル名を入力して、[保存]をクリックする。

重要

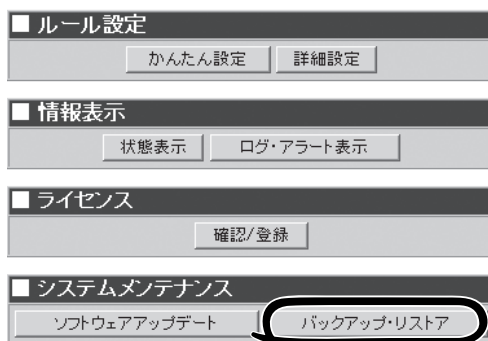
保存したバックアップファイルは、再セットアップ時に使用しますので、大切に保管してください。

セキュリティポリシーのバックアップ

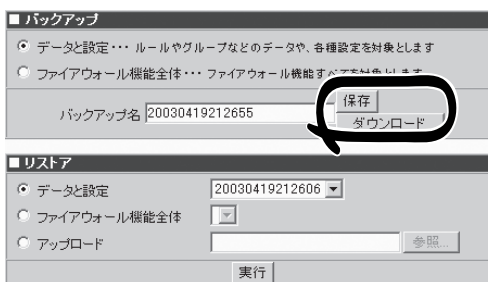
設定したセキュリティポリシーのバックアップを作成します。

Management Consoleから操作しバックアップを行います。Management Consoleへの接続については、4章を参照してください。

1. 画面左側に並ぶメニューアイコンから[ファイアフォール]アイコンをクリックする。

2. [バックアップ・リストア]をクリックする。

   バックアップ・リストア画面が表示されます。

3. バックアップする内容を選択し、バックアップを実行する。

   Express5800/SG300本体へバックアップする場合には、[保存]を、管理クライアントへバックアップする場合には[ダウンロード]をクリックしてください。

   Express5800/SG300本体へバックアップした場合は、しばらくすると、バックアップ・リストアの完了画面が表示されます。

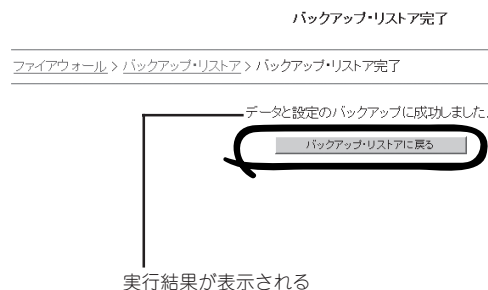
4. 実行結果を確認後、[バックアップ・リストアに戻る]をクリックする。

バックアップ・リストア完了

ファイアウォール > バックアップ・リストア > バックアップ・リストア完了

データと設定のバックアップに成功しました。

バックアップ・リストアに戻る

実行結果が表示される

ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro.sa/doc

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)がインストール済みです。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

シリアル接続の管理PCから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
# export LANG=C
```

システム情報のバックアップ

システムのセットアップが終了した後、オフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。

EXPRESSBUILDER(SE)CD-ROMからシステムを起動して操作します。EXPRESSBUILDER(SE)CD-ROMから起動させるためには、事前にセットアップが必要です。5章を参照して準備してください。

1. 3.5インチフロッピーディスクを用意する。
2. EXPRESSBUILDER(SE) CD-ROMを本体装置のCD-ROMドライブにセットして、再起動する。

   EXPRESSBUILDER(SE)から起動して「EXPRESSBUILDER(SE)トップメニュー」が表示されます。
3. 「ツール」―「オフライン保守ユーティリティ」を選ぶ。
4. [システム情報の管理]から[退避]を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

続いて管理PCに本装置を監視・管理するアプリケーションをインストールします。次ページを参照してください。

二重化構成について

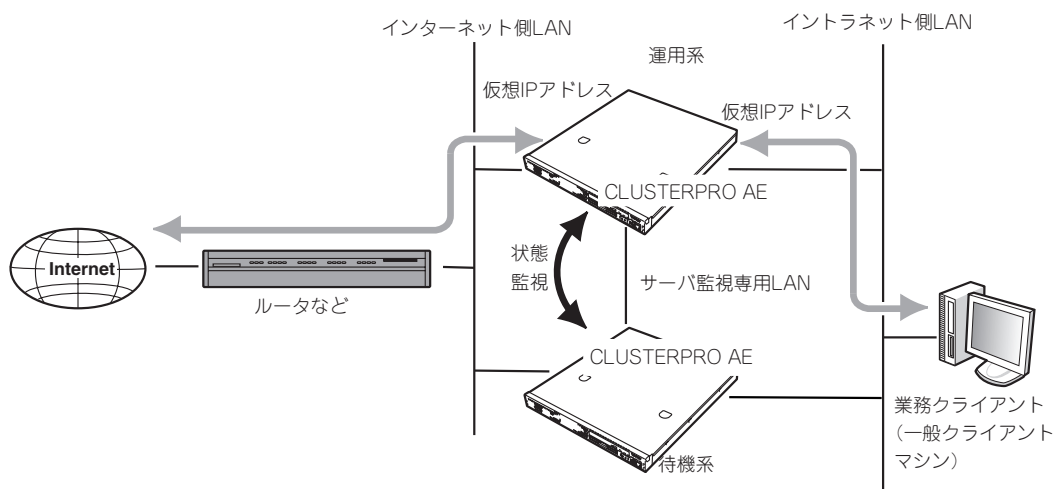
ここではExpress5800/SG300を2台使用して、二重化構成を構築するための手順について説明します。

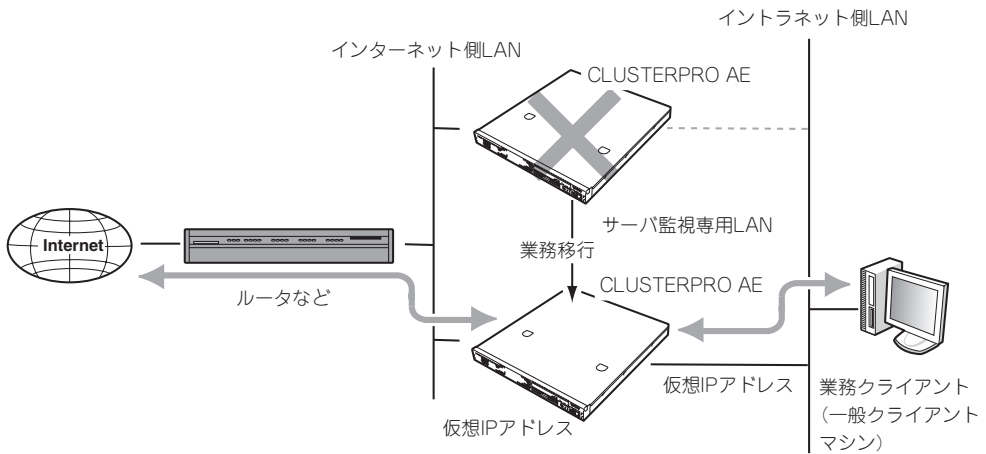
動作概要

Express5800/SG300を二重化することで1台が障害などにより停止しても、もう1台のExpress5800/SG300へ自動的に引き継ぐことにより、障害時の業務停止時間を最小限に抑えることができます。
また、運用系のプロセスの異常を検出した場合や設定されたIPアドレスとの通信が途絶した場合にも、待機系に業務を引き継ぐことが可能です。

以下の仕組みで二重化を実現しています。

- **通常運用時**
  - 運用系側で有効にした仮想IPアドレスを使用してインターネット側とイントラネット側の双方からアクセスします。
  - 運用系と待機系は互いに状態を監視をします。

システムのセットアップ

- **運用系サーバ障害時**
  - 待機系のFirewallが運用系のダウンを検出します。
  - 運用系のFirewallが仮想IPアドレスを無効にします。
  - 待機系のFirewallが仮想IPアドレスを有効にします。
  - インターネット側とイントラネット側の双方からのアクセスは仮想IPアドレスを使用しているため、切り替わり*に伴う設定の変更をする操作を必要としません。

    * 切り替わる前の通信は途絶えます。

DMZを使用する場合もイントラネット、インターネット同様に仮想IPアドレスが引き継がれます。

初期セットアップ

はじめに2台のExpress5800/SG300を二重化構成で動作させるための設定をします。
購入後、初めてのセットアップで二重化構成を使用する場合は、初期導入設定用ディスクを使った初期セットアップの中で、以下に示す項目について設定します。

すでに運用しているExpress5800/SG300を二重化構成にする場合や再度構成し直す場合は、Management Consoleを使用します。詳しい手順については、以下のインターネットホームページで記載しています。参照してください。

http://www.express.nec.co.jp/care/user/InterSec_guide.html

(上記URLが変更された場合には、http://nec8.com/からユーザーズガイド配布ページを参照してください。)

● **設定対象のホストを二重化構成で使用する**

この設定は運用系、待機系の両方で必要な手順です。

二重化構成でExpress5800/SG300を使用するかどうかを設定する項目があります。[設定対象ホストを二重化構成で使用する]にチェックをして、初期導入設定用ディスクを作成してください。

● **ライセンスキーとサポートキーの入力**

運用系と待機系用のライセンスキーとサポートキーを入力します。

運用系と待機系の2つのライセンスキーとサポートキーの入力が必要です。どちらか一方のみを入力すると正しく二重化を構成することはできません。

二重化のための詳細セットアップ

2台のExpress5800/SG300を二重化するためには最低限、次の条件を満たしていないと正しく動作しません。

- 運用系と待機系の二重化基本設定とセキュリティポリシーの設定内容が完全に一致していること（Express5800/SG300本体に割り当てるIPアドレスなどのシステム基本設定は除く）
- 運用系と待機系のライセンスキーとサポートキーがそれぞれのExpress5800/SG300に投入されていること
- 運用系と待機系とも二重化機能サービスが起動していること

運用系と待機系の二重化基本設定とセキュリティポリシーの設定を完全に一致させるために、はじめに一方（運用系）のExpress5800/SG300の基本設定とセキュリティポリシーの設定を完了させ、バックアップ機能を使用して、その内容を任意の場所に保存し、もう一方（待機系）のExpress5800/SG300にリストアします。
次に簡単なセットアップの流れを示します。詳しくは、以下のインターネットホームページで記載しています。参照してください。

http://www.express.nec.co.jp/care/user/InterSec_guide.html

（上記URLが変更された場合には、http://nec8.com/からユーザーズガイド配布ページを参照してください。）

二重化構成をセットアップする場合、および二重化構成を解除する場合（単体サーバとして使用する場合）は、必ず「かんたん設定」をやり直してください。設定の中で仮想IPアドレスなどが正しく設定されていることを確認してください。

スタート

初期導入設定用ディスクによる設定

☞48・75ページ

▽

システムの基本設定

☞60ページ

▽

二重化の詳細設定

☞79ページ

▽

二重化サービスの起動

☞78ページ

▽

状態の確認

[ONLINE]になっていること

☞81ページ

▽

かんたん設定によるセットアップ

[ファイアウォール]→[かんたん設定]

☞4章

▽

ファイアウォールの詳細設定

[ファイアウォール]→[詳細設定]

☞4章

▽

システム情報のバックアップ

[システム]→[バックアップ/リストア]→
任意のバックアップ先
※　基本設定画面での設定内容は含めない

☞69ページ

▽

ファイアウォール設定のバックアップ

[ファイアウォール]→[バックアップ/リストア]→データと設定を選択→任意のバックアップ先

☞71ページ

▽

二重化サービスの停止

☞78ページ

右上に続く

続き ▽

システム情報のリストア

[システム]→[バックアップ/リストア]→
[ファイルを指定してリストア]

☞88ページ

▽

システムの基本設定

☞60ページ

▽

ファイアウォール設定のリストア

[ファイアウォール]→[バックアップ/リストア]→ファイルを選択

☞90ページ

▽

二重化の詳細設定

☞79ページ

▽

二重化サービスの起動

☞78ページ

▽

状態の確認

[ONLINE]になっていること

☞81ページ

▽

二重化サービスの起動

☞78ページ

- [サービス]→[二重化機能]→[詳細設定]→[自動フェイルバック]が[オート]の場合
  <自動フェイルバックが発生>
- [サービス]→[二重化機能]→[詳細設定]→[自動フェイルバック]が[マニュアル]の場合
  <手動で切り替える>

☞84ページ

▽

状態の確認

運用系: [ONLINE]になっていること
待機系: [OFFLINE]になっていること

☞81ページ

■：運用系　■：待機系　□：両系

二重化サービスの(再)起動と停止

二重化サービスの起動、または再起動、停止の方法について説明します。操作画面は、Management Consoleの[サービス]アイコンをクリックすると表示されます。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから[サービス]アイコンをクリックする。

2. [二重化機能]の行の[(再)起動]の項目にある[起動]をクリックする。

   [現在の状態]が[停止中]から[起動中]に、[(再)起動]のボタンが[起動]から[再起動]に切り替わります。

   ヒント

   [OS起動時の状態]でシステムの起動時にサービスの起動を連動させるかどうかを選択することができます。運用する環境に合わせて設定してください。設定を変更した場合は、その設定を有効にするために、[設定]を必ずクリックしてください。

以上でサービスは起動しました。

二重化のサービスをいったん停止する場合は、[停止]をクリックします。
再起動したい場合は、[再起動]をクリックしてください。

[停止]をクリックした場合の例

二重化機能の詳細設定

二重化機能を使用する際に必要なさまざまな設定を変更することができます。設定画面は、Management Consoleの[サービス]アイコンをクリックすると表示されます。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから[サービス]アイコンをクリックする。

2. [サービス]の項目から[二重化機能]をクリックする。

3. [詳細設定]をクリックする。

   詳細設定画面が表示されます。項目と意味については次ページの表を参照してください。

   重要

   二重化設定で割り当てる仮想IPアドレスが、初期導入設定で割り当てたIPアドレスと重複しないよう注意してください。

項　目	説　明
ハートビート送信間隔	ハートビートの送信間隔（秒）を指定します。
ハートビートタイムアウト時間	ハートビートが途絶えて相手側がダウンしたと認識するまでの時間(秒)を指定します。ハートビート送信間隔より大きい値を指定してください。
相手サーバ起動待ち時間	起動時に相手側の起動時間を待ち合わせる時間（秒）を指定します。ハートビートタイムアウト時間より大きい値を指定してください。
内部通信用TCPポート番号	お互いが通信しあうためのTCPのポート番号を指定します。
内部通信用UDPポート番号	お互いが通信しあうためのUDPのポート番号を指定します。
サーバ1ホスト名	ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。
サーバ2ホスト名	
サーバ1のインタコネクトアドレス	相手側を監視するためのアドレスとネットマスクを入力します。
サーバ2のインタコネクトアドレス	
仮想IPアドレス	二重化機能を使用する場合、Express5800/SG300へのアクセスは原則仮想IPアドレスを使用する必要があります。 サーバ間監視専用インタフェースを除く全インタフェースに仮想IPアドレスを設定してください。
監視対象アドレス	監視対象として設定されたIPアドレスとの通信が途絶した場合、待機系にフェイルオーバが行われます。本項目の設定は省略することができます。
運用系サーバ	2台のうちから運用系を指定します。指定しなかった方が、待機系となります。
自動フェイルバック	自動フェイルバックを行うかどうか設定します。自動フェイルバックを「オート」にした場合、運用系ダウン後、待機系に業務が引き継がれ、運用系が復帰（起動）すると、自動的に運用系に業務を戻します。 「マニュアル」にした場合は、Management Consoleから切り替えます。この後の「手動による切り替えとサービスの停止」を参照してください。

4. ［設定］をクリックする。

   操作結果通知で成功の通知があった場合は、［戻る］をクリックして、次の手順に進んでください。何らかのエラーがあるとその内容が表示されます。［戻る］をクリックした後、メッセージに従って設定し直してください。

■ 操作結果通知

二重化設定情報の変更が成功しました。

戻る

状態の確認

二重化を構成しているExpress5800/SG300が互いに正しく通信できているかどうかや、自分自身の二重化に関する状態を確認します。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから[サービス]アイコンをクリックする。

2. [サービス]の項目から[二重化機能]をクリックする。

3. [ステータス確認および二重化切替]をクリックする。

   状態表示画面が表示されます。項目と意味については次ページを参照してください。

「ERROR」や「UNKNOWN」の表示がある場合は、前述の「サービスの起動と詳細設定」で詳細設定の内容を確認し直してください。

ただし、二重化の設定中は、片方が「UNKNOWN」と表示される場合がありますが、設定完了後に表示されていなければ問題ありません。

システムのセットアップ

① 運用系と待機系に付けたサーバ名。先頭にアスタリスク（＊）がついている方が現在状態確認画面を表示中のExpress5800/SG300。

② サーバの状態を示す。
- ONLINE: ハートビートを受信している。
- OFFLINE: ハートビートを受信していない。

③ 二重化を構成するグループとしての状態を表示します(Express5800/SG300で使用するグループはgroup0の1つのみです)。
- ONLINE: 正常
- OFFLINE: 停止
- ERROR: 異常
- UNKNOWN: 不明

④ フェイルオーバポリシを示す。
- 1st: 運用系。
- 2nd: 待機系。

⑤ グループの起動が許可されているかどうかを示す。
- ALLOW: 許可
- DENY: 禁止
- UNKNOWN: 不明

⑥ IPWリソースの起動種別と状態、リソース監視アドレスを示す。
- <A>: 全サーバ起動
- <U>: 単サーバ起動
- ONLINE: 正常
- OFFLINE: 停止
- ERROR: 異常
- UNKNOWN: 不明

⑦ FIPリソースの起動種別と状態、リソース設定アドレスとネットマスクを示す（その他は⑥と同じ）。

⑧ EXECリソースの起動種別と状態、リソース起動/停止時実行パスを示す（以降の表示以外は⑥と同じ）。
- S: 起動時実行パス（監視なし）
- W: 起動時実行パス（監視あり）
- E: 停止時実行パス

フェイルオーバとフェイルバック

二重化構成で運用中、待機側は、運用側のハートビートが詳細設定で決めた時間を超えて途絶えると、運用側が故障したか、または運用側のネットワークに何らかの障害が発生したと認識し、自動的に業務を待機側へと切り替えます(フェイルオーバ)。

元の運用側の障害が取り除かれ、現在の運用側(元の待機側)にハートビートの受信が確立したときは、詳細設定での設定内容に従って運用の切り替え(フェイルバック: 元の運用側への切り戻し)をします。

- **オートの場合**

  自動的に元の運用側に切り替わり、現在の運用側は待機側へと切り替わります。

- **マニュアルの場合**

  Management Consoleを使用して切り替え操作をしない限り切り替わりません。詳しくは、この後の「手動による切り替えとサービスの停止」を参照してください。

運用系サーバにおいて障害を検出した場合には、フェイルオーバが発生し、待機系サーバへ業務が切り替わります。その際に基本設定画面で指定した管理者のE-mailアドレス宛にメールが送信されます。以下に通知されるメッセージの例を示します。

- **ダウンしたときのメッセージ**

```
Subject: WARNING: [group0] is downed
!!WARNING!!
[group0] is not active on Firewall(firewall.nec.co.jp[192.168.1.126]).
Urgently check it.
If you recieved a previous message "NOTICE: [group0] changes
to the active firewall" from firewall.nec.co.jp[192.168.1.126],
both groups are downed.
Urgently check both groups!!
```

- **フェイルオーバしたときのメッセージ**

```
Subject: NOTICE: [group0] chnges to the active firewall
!!NOTICE!!
[group0] chnges to the active
firewall(firewall.nec.co.jp[192.168.1.126]).
Urgently check another failed firewall.
```

重要

- **ダウンした要因がネットワークの通信障害などの場合、ダウンしたときのメッセージがサーバ内に滞留し、障害復旧後に送信されることがあります。メッセージを受信したら必ずその発信時刻を確認するようにしてください。**
- **メールを受信したらExpress5800/SG300の状態を確認し、システムログ(syslog)などからフェイルオーバが発生した要因を確認し、必要な対処を行ってください。メッセージ内容、対処方法等は付録B「二重化機能のログメッセージ」を参照してください。**

監視対象IPアドレスとの通信途絶、またはFirewallモジュールが異常停止し、待機系に業務を引き継いだ場合、以後、そのサーバ上での業務の起動が拒否されるようになります。業務の起動拒否状態は、[サービス]→[二重化機能]→[状態表示] 画面のグループ起動の許可/禁止を示す[STARTING]行で確認することができます。

手動による切り替え

待機側に切り替わった元の運用側をもう一度運用側に手動で切り替えるには、Management Consoleを使用します(詳細設定で自動的に切り替えることもできます)。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから[サービス]アイコンをクリックする。

2. [サービス]の項目から[二重化機能]をクリックする。

3. [ステータス確認および二重化切り替え]をクリックする。

4. 状態表示に「ERROR」や「UNKNOWN」という表示がないことを確認する。

5. [二重化切替]をクリックする。

6. 約10秒後、[最新情報に更新]をクリックして、切り替えが正しく完了していることを確認する。

単体構成への切り替え

二重化構成をやめる場合は、次の手順に従ってください。

1. 待機側のExpress5800/SG300のネットワークケーブルを取り外し、ネットワークから切り離す。

2. 運用側のExpress5800/SG300のManagement Consoleに接続し、左側のメニューから[ファイアウォール]アイコンをクリックする。

3. [ルール設定]の[詳細設定]をクリックし、ファイアウォールメニュー画面し、VPNで二重化の仮想IPを利用しているものを削除する。

4. 運用側のExpress5800/SG300の二重化サービスを停止する。

   78ページを参照してください。

5. 運用側で[ファイアウォール]アイコンをクリックし、[状態表示]をクリックする。

6. [再起動する](または[起動する])をクリックする。

■ 127.0.0.1
現在、正常動作中
停止する
再起動する

7. 運用側で[基本設定]アイコンをクリックし、[基本設定]画面を表示する。

基本設定

8. [二重化機能]のプルダウンメニューを[使用]から[未使用]に切り替え、[設定]をクリックする。

9. 運用側で「かんたん設定」を実行する。

   詳しくは4章を参照してください。

10. 必要に応じて運用側で「詳細設定」を実行する。

   詳しくは4章を参照してください。

11. 必要に応じて待機側も手順2〜10と同様のセットアップをする。

注意・制限事項

- Express5800/SG300 本体が2台必要です。また、ライセンスはそれぞれの実IPアドレスで申請する必要があります。
- 二重化構成でフェイルオーバが発生した場合、接続されていたセッションは切断されます。
- 自動フェイルバックが設定されている場合、運用系サーバの再起動後、自動的に運用系サーバで業務が開始されます。自動フェイルバックが設定されていない場合は、待機系サーバで業務が起動されたままになり、運用系サーバの方が待機状態になります（運用系、待機系の逆転）。運用系サーバに業務を切り替える場合は「手動による切り替え」を参照して切り替えを実行する必要があります。
- 待機系で監視対象IPアドレスとの通信途絶が発生している場合、運用系でリソース異常が発生しても待機系サーバに業務は引き継がれません。ただし、この場合でも「手動による切り替えとサービスの停止」を参照して切り替えることはできます。
- ソフトウェアのアップデートやデータのリストアは待機系、運用系の順番で実行してください。
- 二重化を構成した後、および解除した後は必ず「かんたん設定」を実行してください。また、かんたん設定の中でインタフェースに関する設定が正しいことを確認してください。
- ネットワークを円滑に運用するために、フェイルオーバ後は速やかに障害の原因を取り除き二重化構成に戻してください。

再セットアップ

再セットアップとは、システムの破損などが原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

システムの再インストール

ここでは、システムの再インストールの手順について説明します。

再インストールを行うと、装置内の全データが消去され、出荷時の状態に戻ります。必要なデータが装置内に残っている場合、データをバックアップしてから再インストールを実行してください。

再インストールの準備

Express5800/SG300の電源がOFFの状態で、管理クライアントをExpress5800/SG300背面のLANポートインタフェース(内部ネットワーク用)にクロスケーブルで接続してください。また、内部ネットワークに接続する場合は、ハブなどにLANケーブルで接続してください。

Express5800/SG300との接続に必要なもの

- 管理クライアント
- LANケーブル

再インストールに必要なディスク

- バックアップCD-ROM
- 再インストール用ディスク
- 初期導入設定用ディスク

その他、バックアップしたデータがある場合は、あらかじめ管理クライアント上に準備してください。

再インストール手順

再インストールではExpress5800/SG300本体を再インストールした後、システムの基本情報とポリシールールの再設定を行う必要があります。

システムを新たにセットアップする場合は、システムの再インストールを行った後、前述の「セットアップ」ならびに4章の「かんたん設定ウィザード」を参照して、再度システムの基本設定とセキュリティポリシーのセットアップをしてください。

既存の環境でシステムの基本情報とセキュリティポリシーのバックアップを作成している場合、以下の手順でシステムを既存の環境へ再設定することができます。

システムの再インストール

1. Express5800/SG300の電源をONにし、前面にあるフロッピーディスクドライブに再インストール用ディスクを、CD-ROMドライブにバックアップCD-ROMをセットする。

   自動的にバックアップCD-ROMからのインストールが始まります。
   インストールは約10分で完了します。
   インストールを完了すると、CD-ROMドライブからバックアップCD-ROMが排出されます。
   Express5800/SG300は、電源が入った状態で、システムが停止している状態になります。

2. バックアップCD-ROMおよび再インストール用フロッピーディスクを取り出した後、POWERスイッチを押して電源をOFFにする。

システム基本情報の再設定

1. 初期導入設定用ディスクをセットした後、POWERスイッチを押して電源をONにする。

   初期導入設定用ディスクは、初期導入設定用ツールで作成済みのものを使用してください。

2. しばらく(3分程度)してから、管理クライアントのウェブブラウザを立ち上げ、Management Consoleへ接続し、左側のメニューから[システム]アイコンをクリックする。

   接続については、4章を参照してください。

3. [バックアップ/リストア]をクリックする。

4. ［ファイルを指定してリストア］を選択し、バックアップファイルを指定してリストアする。

5. 左側のメニューの［基本設定］アイコンをクリックし、［設定］をクリックする。

バックアップファイルが反映されます。

バックアップファイルが正常に反映されると、右の画面が表示されます。

6. 左側のメニューの［システム］アイコンを選択し、［システムの再起動］をクリックする。

■ システム管理
バックアップ/リストア...
ログ管理...
syslog監視...
設定確認...
StarDefence連携...
ブリッジ構築支援...
rootパスワード変更...
時刻設定...

■ その他
システム情報...
監査情報...

7. 「システムを再起動します。よろしいですか？」というメッセージが表示されたら、［OK］をクリックする。

8. 再起動画面が表示されたら、［即再起動］をクリックし、再起動する。

セキュリティポリシーのリストア

1. 管理クライアントでブラウザを立ち上げ、Management Consoleへ接続し、左側のメニューから[ファイアウォール]アイコンをクリックする。

2. 画面右側に表示される[バックアップ・リストア]をクリックする。

   バックアップリストア画面が表示されます。

3. リストアするバックアップファイルを選択する。

   Express5800/SG300本体にあるバックアップファイルをリストアする場合は、リストアメニューの「データと設定」のラジオボタンを選択します。右のプルダウンメニューより、バックアップファイルを選択し、[実行]をクリックします。

   管理クライアントにあるバックアップファイルをリストアする場合は、リストアメニューの「アップロード」のラジオボタンを選択します。[参照]をクリックし、バックアップファイルを選択してから[実行]をクリックします。

   [実行]をクリックすると確認メッセージウィンドウが表示されます。

4. [OK]をクリックする。

   しばらくすると、バックアップ・リストア完了画面が表示されます。

5. 実行結果を確認後、[バックアップ・リストアに戻る]をクリックする。

残りのタスク

72ページを参照して、ESMPRO/ServerAgnetのセットアップとマザーボード情報のバックアップを必要に応じて行ってください。